

THREAT AND VULNERABILITY TESTING AND ASSESSMENT (TVTA)

ASC PI Briefing

February 16, 2004

Sandy Landsberg

Office of Research and Development

Science and Technology Directorate

Department of Homeland Security



**Homeland
Security**

TVTA Mission and Objectives

Mission Statement

- Develop, test, and deliver – in collaboration with intelligence, law enforcement, and homeland security community agencies – tools and methodologies for assessing terrorist threats and understanding terrorism.

Strategic Objectives

- Develop **computationally based tools and methodologies** for assessing information about and creating, applying, and disseminating knowledge on terrorist threats and activities
- Determine the motives and intents of and identify terrorists by understanding the socio-political, cultural, economic, and behavioral aspects of terrorism and developing reliable biometric indicators
- Manage directorate-wide activities in analyzing terrorist capabilities for developing and deploying threat agents

TVTA Span of Interest (Influence)

Premises:

risk = f (threat, vulnerability, consequence)

threat = f (*capability*, motive & intent)

Programs:

Capability and Threat Assessment

Motivation and Intent Analysis

Knowledge Management Technologies



Homeland
Security

TVTA Capabilities

Knowledge Management Technology

- Data Representation – Data Sciences and Semantic Graph Techniques
- Visualization and Analytics - National Visualization and Analytics Center (NVAC)
- Modeling, Simulation, and Discrete Sciences - Institute for Discrete Sciences (IDS)
- Testing and Evaluation - Interagency Center for Applied Homeland Security Technology (ICAHST)

Motivation and Intent

- Socio-political, Cultural, Behavioral, and Economic Indicators
- Biometrics – Identification, Validation, Deception Detection

Specialized Intelligence Assessment

- all-WMD Capability Assessments
- S&T Threat Assessments*
- Nuclear Assessment Program (FY 2005 only)



Homeland
Security

Needs Assessment

TVTA addresses the full spectrum of needs faced by DHS, for which it must develop tools in these areas:

- **Threat Assessment:** Create and establish coherent capabilities for analysis, dissemination, visualization, insight, synthesis, and enhancement of terrorism-related information
- **Data Sharing:** Enable tactical and strategic sharing of terrorism-related intelligence, information, and data among all elements of the homeland security community
- **Forecasting:** Identify, understand, and forecast terrorist motives, intentions, behaviors, capabilities, processes, and tactics; understand individual and societal resilience to terrorism
- **Scalable Analyses:** Enable scalable, integrated simulation and information analyses for threat identification and assessment; develop innovative computational technologies for deployment in next-generation knowledge management and threat assessment tools
- **System Optimization:** Create optimized knowledge system designs and architectures that enhance the nation's countermeasures

Information Analysis (IA) Needs

IA Requirements	Threat Assessment	Data Sharing	Forecasting	Scalable Analysis	Systems Optimization
High-volume Ingestion	H			H	H
Computing Infrastructure	H	H	M	H	H
Embedded and Configurable Analysis	M	M	M	M	H
Entity Extraction	H			H	L
Event Detection	H			H	L
Unstructured Data and Information	H	M	H	H	M
Vetting of Sources	L	L			L
New COTS and GOTS Systems	L	L	L		
Performance Metrics	L		L	L	L
Collaborative Environment	H	H	H	H	L
Self-Learning Statistics	L		L	L	
Database Consolidation	L	L			M
Common Operating Picture	M	M	L		M



**Homeland
Security**

H – High level of involvement
M – Medium level of involvement
L – Low level of involvement

Information Analysis (IA) Needs

IA Requirements	Threat Assessment	Data Sharing	Forecasting	Scalable Analysis	Systems Optimization
Data Acquisition Modeling and Predictive Analysis	H		H	H	
Community of Interest Database	H	H			M
Unified Information Portal	L	L			L
State and Local Information Centers	L	L			
4-D Modeling and Simulation for Cities and Infrastructures	H		H	M	M
Business Intelligence	M		L	L	
Predicting Future Threats	H		H	H	

H – High level of involvement
 M – Medium level of involvement
 L – Low level of involvement



**Homeland
Security**

Other DHS Components Needs

Directorate	Threat Assessment	Data Sharing	Forecasting	Scalable Analysis	Systems Optimization
BTS					
Automated scene understanding for borders	M	M		M	M
Sensor and intelligence fusion	H	M	L		M
Common Operating Picture for border grid	H	H			M
Threat/vulnerability prediction for transportation systems	L	L	L	M	
Intelligence sharing	H	H	H		
Multi-modal database access	H	H		H	H
Common Operating Environment	H	H			M
Intelligence fusion and prediction system	H	H	H	M	
EP&R					
Integrated information technology framework	M	H		M	H
Management of distributed data sources	M	H		M	M
Archived incident and exercise information	L	L	L	L	



**Homeland
Security**

H – High level of involvement
M – Medium level of involvement
L – Low level of involvement

Other DHS Components Needs

Directorate	Threat Assessment	Data Sharing	Forecasting	Scalable Analysis	Systems Optimization
EP&R					
Information security		L			L
Real time access to and synchronization of distributed data sources	H	H		M	H
Modeling & simulation for training & exercising incidents	M		M	H	
Architectures for massive, gaming technology for emergency exercises		M		M	M
Interagency Modeling and Atmospheric Analysis Center	H	H		H	
USCG					
Situational Awareness and Assessment Tools	H	H	H	L	
Vessel Detection and Assessment Tools	L	L		L	
Real-time Personnel Identification	H	H			M
USSS					
Analysis of changing attack trends, methodologies, mediums, etc.	H	L	M	L	
CBRNE					
Detection of chemical, biological, radiological and nuclear, and explosive threats in various protection scenarios	M	M	M	M	
Central command and control of threat information in real time	M	M			L



**Homeland
Security**

H – High level of involvement
M – Medium level of involvement
L – Low level of involvement

Capability: Knowledge Management Technology

Modeling, Simulation, and Discrete Sciences

Current Capabilities

- Large scale integration and querying capability first integrated into BKC's Biodefense Encyclopedia with initial interfaces to 15 genomics and proteomics databases
- Parallel 2D-hypergraph partitioning reduced communication 10-100X for semantic graph querying and analysis in support of threat characterization
- Delivered 10X speedup in DNA signature algorithm and development of first draft-sequence alignment algorithm for improved pathogen detection
- Reduced grid generation time 5000X via a novel and automated adaptive cut-cell approach that provides IMAAC with essential new capabilities for urban dispersion modeling
- Coupled flow/transport simulations and optimization techniques to locate a contaminant source from sensor data
- Developed a discrete agent-based simulation framework for analyzing how terrorist acts affect the financial sectors and to help understand which mitigation and response strategies are most effective.

Interim Capabilities

- Engage academia and industry in collaborative discrete sciences R&D to deliver 100x improvement in feasible problem size and time-to-solution for ADVISE and BKC deployment
- Develop new tools to automate data ingest and distributed graph algorithms that demonstrate 100x improvement in throughput and response time
- Develop a software framework that integrates various simulations into a single environment for threat assessment and training
- Define and develop an infrastructure for knowledge networking and information sharing among massive, distributed, disparate information sources (collaboration with ADVISE)

Desired Capability End-State

- Establish enduring, nation-wide capabilities for research in science and technology areas critical to threat and vulnerability assessment through an Institute for Discrete Sciences supported by a complex of university, industry, and government laboratories.
- Deliver scalable discrete math and uncertainty quantification algorithms to enable large-scale multi-simulation and information analyses with confidence measures
- Deliver algorithms and tools that enable continuous high-throughput data ingest and analysis on large-scale parallel computers; establish DHS computing resources for research and development in support of operational assets
- Deliver scalable, integrated simulation analyses with knowledge management tools for threat assessment, decision support, scenario planning and incident response

Residual Risk

- Uncertainty regarding appropriate high-performance hardware platforms for large-scale knowledge management technologies for DHS customers

ASC Cross-Cut

- **FY05/FY06 Plan to address multiple portfolio needs**
 - BioCM, Rad/Nuc CM, Chem CM, CIP, EP&R, BTS
- Computational tools and methodology in support of All-Threat Knowledge Center
 - Help meet the needs of the rapidly-expanding Biodefense Knowledge Center both in operational environment and longer-term research and development
 - Help provide integration and interoperability to extensive databases, models, systems, and networks
- Multi-simulation
 - Provide integration framework for discrete and continuous simulations
 - Provide improved algorithms and models for increased accuracy and turn-around time





Homeland Security



Homeland
Security